UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/058,661	01/28/2002	James F. Riordan	CH9-2000-0011	8370

29683 7590 01/24/2006

HARRINGTON & SMITH, LLP
4 RESEARCH DRIVE
SHELTON, CT 06484-6212

EXAMINER	
CERVETTI, DAVID GARCIA	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 01/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/058,661	RIORDAN ET AL.	
	Examiner	Art Unit	
	David G. Cervetti	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 November 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's arguments filed November 7, 2005, have been fully considered but they are not persuasive.

2. Claims 1-13 are pending and have been examined.

Response to Amendment

3. The objection to the drawings is withdrawn.

4. The objection to the abstract is withdrawn.

5. The objection to disclosure regarding the terms not defined is withdrawn.

6. The rejection of claims 9 and 12 under 35 USC § 112 is withdrawn.

7. Claims 1, 3, 5, 7-8, 10-11, and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher et al. (US Patent Number: 6,327,661, hereinafter Kocher), and further in view of Tschudin (NPL Apoptosis – the Programmed Death of Distributed Services").

8. Claims 2, 4, 6, 9, 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher and Tschudin, and further in view of Esserman et al. (US Patent Number: 5,144,664, hereinafter Esserman).

9. Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

10. Applicant's arguments do not comply with 37 CFR 1.111(c) because they do not clearly point out the patentable novelty which he or she thinks the claims present in view

of the state of the art disclosed by the references cited or the objections made. Further, they do not show how the amendments avoid such references or objections.

11. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

12. Applicant admits in the Remarks that the only allegedly missing feature from the prior art is checking by using a test plaintext/ciphertext. Assuming arguendo Applicant is correct, is still checking, checking information for validating input/output on an information processing device was conventional and well known. **However, Tschudin clearly teaches checking using test values (page 258), namely "for each presented key we attempt to decrypt the ENCRYPTED_CODE. Looking at the result we can decide if this was a valid decryption or not.**" (emphasis added).

13. An apoptosis key, as disclosed, is nothing more than a key that has been changed (dead, expired, not in use, etc). Thus, it would have been obvious to someone of ordinary skill in the art to check if an expired key is being used.

14. Checking whether an expired key has been used to attempt access to a computer system is conventional and well known. Authentication methods for computer systems prompting users to change a password (key) after a certain amount of time had passed, were conventional and well known at the time the invention was made. It was also conventional and well known to prevent the re-use of a certain key by a certain

user. This necessarily implies that an old key was saved to verify the user did not attempt to use the same key at a later time.

15. In response to Applicant's request for a reference that teaches publishing information, Examiner submits US Patent 4,634,807 to Chorley et al. (hereinafter Chorley). Chorley teaches publishing a plaintext message and its corresponding encrypted text (column 3, lines 1-67).

Claim Rejections - 35 USC § 103

16. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

17. Claims 1, 3, 5, 7-8, 10-11, and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher, and further in view of Tschudin.

Regarding claim 1, Kocher teaches a cryptographic system comprising first cryptographic algorithm means for enabling cryptographic operations (column 2, lines 60-67, column 13, lines 20-67), input/output means for receiving input streams and sending output streams (column 13, lines 20-67, column 14, lines 61-67), wherein said input streams are transformed to said output streams by said cryptographic operations (column 13, lines 20-67), at least one test plaintext P_i and for each test plaintext P_i a corresponding test ciphertext C_i (column 13, lines 20-67), receiving means for receiving a control stream (column 13, lines 20-67, column 14, lines 1-60), checking means for checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under the cryptographic operation of said first cryptographic algorithm means (column 13, lines 20-67), switching means for stopping

said cryptographic operations with said first cryptographic algorithm means (column 13, lines 20-67), wherein said stopping by said switching means is triggered by said checking means (column 13, lines 20-67). Kocher does not expressly disclose including at least one apoptosis key K_i. Kocher teaches self-destructing keys. However, Tschudin teaches the concept of "apoptosis" related to distributed services and computer security (sections 3-5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use an "apoptosis key". One of ordinary skill in the art would have been motivated to perform such a modification to control the execution of services (Tschudin, sections 4-5).

Regarding claim 3, the combination of Kocher and Tschudin teaches the limitations as set forth under claim 1 above. Furthermore, Kocher teaches said receiving means is made for accepting control streams which include at least one plaintext P_i, for each plaintext P_i a corresponding ciphertext C_i (column 2, lines 60-67, column 3, lines 1-10) and said checking means is made for trying to find a test plaintext P_i and a test ciphertext C_i equal to said received plaintext P_i, wherein said checking is done with said apoptosis key of said equal test plaintext P_i and said equal test ciphertext C_i (column 13, lines 20-67, column 14, lines 61-67) and Tschudin teaches the concept of "apoptosis" related to distributed services and computer security (sections 3-5).

Regarding claim 5, Kocher teaches a method for creating a cryptographic system for carrying out cryptographic operations characterized by the steps of implementing within said cryptographic system a first cryptographic algorithm enabling said cryptographic operations (column 2, lines 60-67, column 3, lines 1-10), selecting at

least one test plaintext P_i and enciphering each test plaintext P_i with said first cryptographic algorithm thereby generating a corresponding test ciphertext C_i for each test plaintext P_i (column 2, lines 60-67, column 13, lines 20-67), implementing within said cryptographic system said at least one test plaintext P_i and for each test plaintext P_i said corresponding test ciphertext C_i (column 13, lines 20-67, column 14, lines 61-67), implementing within said cryptographic system receiving means for receiving a control stream (column 13, lines 20-67, column 14, lines 61-67), implementing within said cryptographic system checking means for checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under said first cryptographic algorithm (column 13, lines 20-67), implementing within said cryptographic system switching means for stopping said cryptographic operations with said first cryptographic algorithm (column 13, lines 20-67), wherein said stopping by said switching means is triggered by said checking means (column 13, lines 20-67). Kocher does not expressly disclose the use of one apoptosis key K_i. Kocher teaches self-destructing keys. However, Tschudin teaches the concept of "apoptosis" related to distributed services and computer security (sections 3-5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use an "apoptosis key". One of ordinary skill in the art would have been motivated to perform such a modification to control the execution of services (Tschudin, sections 4-5).

Regarding claim 7, the combination of Kocher and Tschudin does not expressly disclose publishing said at least one test plaintext P_i and for each test plaintext P_i said

corresponding test ciphertext C_i. However, Examiner takes Official Notice that publishing information was conventional and well known at the time the invention was made. Furthermore, Kocher stores plaintext and ciphertext prior to comparing them. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to publish this information since Examiner takes Official Notice that it was conventional and well known.

Regarding claim 8, Kocher teaches a method for operating a cryptographic system for carrying out cryptographic operations (column 2, lines 60-67, column 3, lines 1-10) characterized by the steps of providing a first cryptographic algorithm for enabling said cryptographic operations (column 2, lines 60-67, column 13, lines 20-67), receiving input streams and sending output streams wherein said input streams are transformed to said output streams by said cryptographic operations (column 13, lines 20-67, column 14, lines 61-67), receiving a control stream, checking whether a test ciphertext C_i is the enciphered image of a corresponding test plaintext P_i under said first cryptographic algorithm when using said key K_i (column 13, lines 20-67), stopping said cryptographic operations with said first cryptographic algorithm, if said test ciphertext C_i is the enciphered image of said corresponding test plaintext P_i under said first cryptographic algorithm (column 13, lines 20-67). Kocher does not expressly disclose the use of one apoptosis key K_i. Kocher teaches self-destructing keys. However, Tschudin teaches the concept of "apoptosis" related to distributed services and computer security (sections 3-5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use an "apoptosis key". One of ordinary skill in the art

would have been motivated to perform such a modification to control the execution of services (Tschudin, sections 4-5).

Regarding claim 10, the combination of Kocher and Tschudin teaches the limitations as set forth under claim 8 above. Furthermore, Kocher teaches wherein said receiving of a control stream includes for each key K_i receiving of a plaintext P_i and a corresponding ciphertext C_i (column 2, lines 60-67, column 3, lines 1-10), and said checking includes trying to find a test plaintext P_i and a test ciphertext C_i equal to said received plaintext P_i, and said received ciphertext C_i wherein said checking is done with said key of said equal test plaintext P_i and said equal test ciphertext C_i (column 13, lines 20-67, column 14, lines 61-67) and Tschudin teaches the concept of "apoptosis" related to distributed services and computer security (sections 3-5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use an "apoptosis key". One of ordinary skill in the art would have been motivated to perform such a modification to control the execution of services (Tschudin, sections 4-5).

Regarding claim 11, Kocher teaches a computer software product for operating a cryptographic system for carrying out cryptographic operations (column 14, lines 5-60), said product is characterized by a computer-readable medium in which program instructions are stored (column 14, lines 5-60), which instructions, when read by a computer, enable the computer to perform a first cryptographic algorithm that is enabling said cryptographic operations (column 2, lines 60-67, column 3, lines 1-10), receive input streams and send output streams wherein said input streams are

transformed to said output streams by said cryptographic operations (column 13, lines 20-67, column 14, lines 61-67), receive a control stream which is including at least one key K_i, check whether a test ciphertext C_i is the enciphered image of a corresponding test plaintext P_i under said first cryptographic algorithm when using said key K_i, stop said cryptographic operations with said first cryptographic algorithm (column 13, lines 20-67), if said test ciphertext C_i is the enciphered image of said corresponding test plaintext P_i under said first cryptographic algorithm when using said key K_i (column 13, lines 20-67). Kocher does not expressly disclose the use of one apoptosis key K_i. Kocher teaches self-destructing keys. However, Tschudin teaches the concept of "apoptosis" related to distributed services and computer security (sections 3-5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use an "apoptosis key". One of ordinary skill in the art would have been motivated to perform such a modification to control the execution of services (Tschudin, sections 4-5).

Regarding claim 13, the combination of Kocher and Tschudin teaches the limitations as set forth under claim 8 above. Furthermore, Kocher teaches computer program comprising program code means for performing the steps of claim 8 when said program is run on a computer (column 14, lines 5-60).

18. Claims 2, 4, 6, 9, 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher and Tschudin, and further in view of Esserman.

Regarding claim 2, the combination of Kocher and Tschudin does not expressly disclose at least one second cryptographic algorithm means, wherein said switching

means enables switching to said at least one second cryptographic algorithm means. However, Esserman teaches at least one second cryptographic algorithm means, wherein said switching means enables switching to said at least one second cryptographic algorithm means (column 4, lines 1-41). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to switch between multiple encryption algorithms when an encryption algorithm is compromised. One of ordinary skill in the art would have been motivated to perform such a modification to maintain secure communications (Esserman, column 1, lines 39-67, column 2, lines 1-68).

Regarding claim 4, the combination of Kocher and Tschudin does not expressly disclose a cascaded list of different cryptographic algorithm means. However, Esserman teaches a cascaded list of different cryptographic algorithm means (column 4, lines 1-41). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a cascaded list of different cryptographic algorithm means. One of ordinary skill in the art would have been motivated to perform such a modification to maintain secure communications (Esserman, column 1, lines 39-67, column 2, lines 1-68).

Regarding claim 6, the combination of Kocher and Tschudin does not expressly disclose implementing within said cryptographic system at least one second cryptographic algorithm for said ciphering operations, and switching by said switching means to said at least one second cryptographic algorithm. However, Esserman teaches implementing within said cryptographic system at least one second

cryptographic algorithm for said ciphering operations, and switching by said switching means to said at least one second cryptographic algorithm (column 4, lines 1-41). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use at least one second cryptographic algorithm for said ciphering operations, and switching to a second cryptographic algorithm. One of ordinary skill in the art would have been motivated to perform such a modification to maintain secure communications (Esserman, column 1, lines 39-67, column 2, lines 1-68).

Regarding claim 9, the combination of Kocher and Tschudin does not expressly disclose switching to one of said second cryptographic algorithms for said cryptographic operations after said stopping. However, Esserman teaches switching to one of said second cryptographic algorithms for said cryptographic operations after said stopping (column 4, lines 1-41). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a second cryptographic algorithm for said ciphering operations, and switching to a second cryptographic algorithm. One of ordinary skill in the art would have been motivated to perform such a modification to maintain secure communications (Esserman, column 1, lines 39-67, column 2, lines 1-68).

Regarding claim 12, the combination of Kocher and Tschudin does not expressly disclose computer software product, wherein said instructions, when read by a computer, enable the computer to perform at least a second cryptographic algorithm and switch to said at least one second cryptographic algorithms for said cryptographic

operations after said stopping. However, Esserman teaches computer software product, wherein said instructions, when read by a computer, enable the computer to perform at least a second cryptographic algorithm and switch to said at least one second cryptographic algorithms for said cryptographic operations after said stopping (column 4, lines 1-41). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a second cryptographic algorithm for said cryptographic operations, and switching to a second cryptographic algorithm. One of ordinary skill in the art would have been motivated to perform such a modification to maintain secure communications (Esserman, column 1, lines 39-67, column 2, lines 1-68).

Conclusion

19. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Pearson et al. (US Patent 5,838,256) teach detecting use of an expired key. Rehm (US Patent 5,740,243) teaches publishing plaintext/ciphertext pairs.

20. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

21. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

22. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

23. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DGC

Primary Examiner
AU 2131
1/21/06